Report Purpose and Scope

This Report was prepared as required by Assembly Bill 2231 (Pavley, Government Code Section 8593.6). The legislation required that the Office of Emergency Services (OES) convene a Working Group "to develop policies and procedures that will provide a framework for instituting a public-private partnership with providers of mass communications systems to enhance public access to emergency alerts". The Working Group was also tasked with "assessing existing and future technologies available in the public and private sectors for the expansion of transmission of emergency alerts to the public" and to provide advice to the OES Director on development of policies and procedure that "will lay the framework for an improved warning system for the public".

Specifically, the statute requires the Working Group to consider and make recommendations with respect to all of the following:

- Private and public programs, including pilot projects that attempt to integrate a public-private partnership to expand an alert system.
- Protocols, including formats, source or originator identification, threat severity, hazard description, and response requirements or recommendations, for alerts to be transmitted via an alert system that ensures that alerts are capable of being utilized across the broadest variety of communication technologies, at state and local levels.
- Protocols and guidelines to prioritize assurance of the greatest level of interoperability for first responders and families of first responders.
- Procedures for verifying, initiating, modifying, and canceling alerts transmitted via an alert system.
- Guidelines for the technical capabilities of an alert system.
- Guidelines for technical capability that provides for the priority transmission of alerts

.

- Guidelines for other capabilities of an alert system.
- Standards for equipment and technologies used by an alert system.
- Cost estimates.
- Standards and protocols in accordance with, or in anticipation of, Federal Communications Commission requirements and federal statutes or regulations.
- Liability issues.

Alert and Warning Background

> *"Timely and effective public warnings can save lives, reduce property losses and speed economic recovery. Public warning empowers citizens by providing them with the information they need during times of emergency to make informed decisions. The objective of a public warning system is to capture the attention of people at risk, to provide them with relevant and accurate information regarding the nature of the threat and to provide such information in time for protective actions to be taken. A truly effective public warning system will reach those at risk regardless of their location, time of day or night or any disabilities or special needs."*
>
> Partnership for Public Warning, Protecting America's Communities, June 2004

The process of issuing a public alert or warning includes several key elements:

- Evaluating the emergency situation and identifying/assessing the risk
- Deciding to issue a warning
- Crafting the warning message
- Disseminating the warning
- Validating the warning
- Taking action on the warning.

Alert and warning policies and procedures, including guidelines for when a warning should be issued and who is able to issue a warning, need to be developed ahead of time and included in jurisdiction Emergency Operations Plans. The public must also be educated about available alerting and warning systems and appropriate action to take when a warning is received. Alerting systems must also be tested regularly and tests evaluated to provide feedback for system improvements.[1]

It is important to differentiate "alert and warning" from "public information". Making a recommendation to the Incident Commander/Emergency Manager regarding issuance of an alert is an Operations Section function. Issuing an alert is an initial response action, requiring rapid decision-making, often in an environment of uncertainty. The alert will often refer recipients to public information sources (e.g., press releases, internet postings) for follow-up information.

[1] Partnership for Public Warning, Protecting America's Communities: An Introduction to Public alert and Warning, June 2004 (PPW Report 2004-2)

There has been considerable academic research on public response to alerts and warnings.[2] There are several "myths" related to public reaction to warnings:

- Panic (people do not panic in response to warnings, particularly well worded warnings),
- Keep it simple (actually, recipients want a lot of accurate information in the warning message, if not they will search for it from other sources), and
- False alarms (while an adequately explained false alarm may not deter future behavior, irrelevant alarms may have this effect – the "car alarm" syndrome.)

The elements of the warning message are key in influencing the public to take the proper response:

- The message should come through multiple, diverse channels;
- The more it is repeated and heard the better;
- The content should include what to do, when to do it, who should do it, why they should do it, and who is making the recommendation;
- The message style should be clear, specific, accurate, certain, and consistent;
- The warning should come from a credible source; as credibility may vary between elements of the population to be warned, a panel or multiple sources should be used.

Most recipients will want to validate the information before taking action. The message should refer recipients to preferred sources (e.g., tune to your local radio station, reference an official website, refer them to 2-1-1 or 3-1-1 operators); if not they will call 9-1-1.

National Alert and Warning Initiatives

There are several on-going alert and warning initiatives at the national level:

Common Alerting Protocol (CAP)

The objective of the Common Alerting Protocol (CAP) is to define "a single message format with the essential features to handle existing and emerging alert systems and sensor technologies."[3] CAP was adopted by the Organization for the Advancement of Structured Information Standards (OASIS) in 2004. CAP allows the sender of an alert message to activate many types of warning systems with a single input, thus ensuring a common message is sent to as many warning devices as possible. In structuring

[2] Information in the following paragraphs derived from Dennis S. Mileti and Erica Kuligowski, "Public Warnings and Response: Research Findings and Evidence Based Applications for Practice", Power Point presentation (revision 12C), no date

[3] CAP Fact Sheet, CAP Cookbook, www.incident.com

the message format protocol the standards crafters based the template on findings of academic research and real-word events. The structure includes four general groups of message components[4]:

- Alert: This group of message elements includes such essential elements as the originator of the message, the date/time it was sent, its status (e.g., actual warning, exercise warning, system test), scope (e.g., public audience, restricted audience, or private), and message type (e.g., alert, update, cancel).
- Info: This group of message elements includes the event, urgency of the event/alert (e.g., action should be taken immediately, soon, or near future), severity of the event (e.g., extreme, severe, moderate, minor), and certainty of occurrence (e.g., very likely, likely, possible, unlikely).
- Resource: Allows for inclusion of additional information to enhance the elements under the "Info" section.
- Area: A text description of the impacted area.

Commercial Mobile Alert System (CMAS)

In April 2008, the Federal Communications Commission (FCC) adopted the Commercial Mobile Alert System (CMAS), a system by which mobile service (e.g., cellular telephone) providers can relay authenticated emergency messages and alerts to their mobile device customers. The creation of the system was mandated by the Warning Alert Response Network (WARN) Act. Participation in the CMAS is voluntary on the part of commercial mobile service (CMS) providers. Customers would automatically receive a text message alert when issued by their provider. Messages will be targeted to the County level.

A key role in the functioning of the CMAS is the "Alert Aggregator". According to the FCC summary of CMAS[5], the Alert Aggregator "would receive, authenticate, validate and format Federal, state, tribal and local alerts and then forward them to the appropriate CMS Provider Gateway. The CMS Provider Gateway and associated infrastructure would process the alerts and transmit them to subscriber handsets." Until recently, it had been unclear which federal agency would take on this Alert Aggregator role. However, on May 30, 2008 the Federal Emergency Management Agency (FEMA) announced that it would take on the Alert Aggregator role, subject to several conditions. Of particular interest to the State, FEMA indicated that "the federal Aggregator will interface, but not interfere with, existing state and local alerting systems" and that "states would be responsible for determining and identifying those persons who have the authority to send alerts for their specific jurisdictions". According to the FEMA release, the system by which this Alert Aggregator would perform its function has not been designed or

[4] OASIS Common Alerting Protocol, v. 1.0, p. 9-19, describes all required and optional message components.

[5] Federal Communications Commission, Public Safety and Homeland Security Bureau website, "Mobile Telephone Alerts"

engineered.[6] Although CMAS was designed to integrate with CAP, in the same release, FEMA noted that it would “announce its position on adopting” CAP by the end of July 2008.

Integrated Public Alert and Warning Systems (IPAWS) and the Emergency Alert System (EAS)

In June 2006 President Bush issued an Executive Order stating that it is the policy of the United States’ to have “an effective, reliable, integrated, flexible and comprehensive system to alert and warn the American people.”[7] The Integrated Public Alert and Warning System (IPAWS) is a federal public-private initiative, coordinated by Department of Homeland Security/FEMA, to address this mandate. It is to establish “next generation public communications and warning capability…to allow the President and authorized officials to effectively address and warn the public and State and local emergency operations centers via phone, cell phone, pagers, computers and other personal communications devices.”[8] It will use digital technology to send emergency alert data to a variety of media and devices. It will allow messages to be transmitted in audio, video, and text and in multiple languages including American Sign Language and Braille.[9]

IPAWS primarily updates the existing Emergency Alert System, which relies on broadcast television and radio, and National Oceanic and Atmospheric Administration Weather Radio Network. FEMA is statutorily responsible for the EAS and has designated the FCC to coordinate broadcaster participation. (Broadcasters are mandated to participate in national level alerts but participation in State and local level alerts are voluntary. However, this has not been a problem in California.) Under the current EAS, the alert messages are relayed to the “Primary Entry Point”, who then relays it to other radio and television stations for rebroadcast.[10] (Due to its size, California has a primary [KCBS, San Francisco] and secondary [KFWB, Los Angeles] “Primary Entry Point, and a designated “State Entry Point [KFBK, Sacramento].[11])

[6] Federal Emergency Management Agency, “FEMA to Assume Aggregator/Gateway Role for nationwide Cell Phone Alert System”, May 30, 2008, release number HQ-08-090

[7] Executive Order 13407, “Public Alerts and Warning System”, signed by President George W. Bush, June 26, 2008.

[8] Federal Emergency Management Agency website, “Integrated Public Alert and Warning System”, “What is IPAWS?”

[9] Federal Emergency Management Agency website, “Integrated Public Alert and Warning System”, “What IPAWS Does”

[10] Memorandum from Committee on Transportation and infrastructure Oversight and Investigations Staff to Members of the Subcommittee on Economic Development, Public Buildings, and Emergency Management, Subject: Hearing on “Assuring Public Alert Systems Work to Warn American Citizens of natural and Terrorist Disasters”, June 3, 2008, pages 1-2.

[11] State of California Emergency Alert System, State EAS Plan, November 2002.

The United State House of Representatives Subcommittee on Economic Development, Public Buildings, and Emergency Management held a hearing on June 4, 2008 that addressed the status of IPAWS. It noted that FEMA is conducting 14 pilot projects throughout the nation to develop various aspects of the IPAWS. The staff report[12] notes that many of the pilot projects are concluding, yet there does not seem to be a clear plan and timeline for IPAWS implementation.

Follow-up legislation, the "Integrated Public Alerts and Warning Systems Modernization Act of 2008" (H.R. 6038) was introduced in the US House of Representatives in May 2008. It amends the Robert T. Stafford Act to direct the President to modernize the alert and warning system. It memorializes in statute much for the current IPAWS, CAP, and CMAS initiatives and the directives of the Executive Order 13407.

State Level Alerting and Warning History

Emergency Digital Information Service (EDIS)

The Emergency Digital Information Service (EDIS) is a "state operated public warning system that links emergency managers to the news media, public, and other agencies. It is part of the state's Emergency Alert System and is available without charge to local, state, and federal agencies serving California."[13] EDIS has been in operation since 1990 and provides text-based information to news media, emergency managers, and other users via the Internet to email, computer desktop, or text-enabled mobile devices. EDIS can also be used to transmit warning messages to the EAS, which then broadcasts them to the public via television or radio. EDIS is fully compatible with CAP, enabling "plug and play" with other CAP compliant means of issuing alerts and warnings. Messages are created on the Internet, allowing authorized operators to create them at any location with Internet access. EDIS has the capability to work with Geographic Information Systems to target warning delivery. EDIS can be enhanced to serve a broader role in an expanded alert and warning system in California.

Survey of Existing Alert and Warning Systems Used in California (OES Technology Contract)

The Governor's Office of Emergency Services (OES) is soliciting offers for services to assist with the development of a statewide strategy for enhancement of systems and protocols for alerting the general public and public officials of potential emergencies ranging from tsunamis to chemical spills. The intent is for the contractor to:

[12] See footnote 8, pages 4-5

[13] California Governor's Office of Emergency Services, Emergency Digital Information Service Fact Sheet (no date).

- Create a state strategy for multi-year improvement of the technology, protocols, and policies for notifying the public and public officials in emergency situations of actions necessary to relocate themselves or take other protective measures.
- Provide technical assistance to OES and its various advisory committees relative to the development and implementation of emergency alert and warning systems.
- Create a training curriculum that will aid emergency personnel in effectively using alert and warning systems.

CA-OES is currently going through the process of hiring a consultant to accomplish this task. There are currently six proposals that are being considered. However, the contract cannot be finalized before the State budget is signed.

Assembly Bill 2393

AB 2393 (Levine), regarding telecommunications and emergency service, requires the California Public Utilities Commission (CPUC) to investigate certain aspects of alert and warning via telephone devices. This effort recognizes the growing importance of mobile telephones and the growing number of Californians who rely ***exclusively*** on mobile service for voice telecommunications.

Because of its standing as a leader in emergency communications, large population, and unique topographical and demographic challenges, California is ideally suited to test this technology through a First Office Application (FOA), the goal of which will be to identify obstacles, solutions and best practices for a nationwide rollout of the Commercial Mobile Alert System (CMAS). Under the FOA proposal, the California Public Utilities Commission, and the Governor's Offices of Emergency Services and Homeland Security will work together to design, implement and evaluate a state-wide test of CMAS.

AB2393 is legislative mandate directing the CPUC has to investigate current capabilities, best practices and the value of establishing standards for emergency alerting in California. To that end, the CPUC has held a 2007 emergency alerting workshop and in January 2008 a Southern California firestorm workshop. The CPUC Communications Division is now investigating the impact of the fires on communication networks; with emphasis on network response and recovery and the performance of emergency notification systems. Under this initiative:

1) The PUC is to consider the need for performance reliability standards for backup power systems installed on the property of residential and small commercial customers by a facilities-based provider of telephony services. This law also requires PUC to investigate the need for telecommunications service systems not on the customer's premises to have backup electricity to enable telecommunications networks (911) to function and to enable the customer to contact a public safety answering point operator during an electrical outage.

2) The PUC, in consultation with OES and DGS, is to investigate whether standardized notification systems and protocols should be utilized to facilitate notification of affected members of the public of local emergencies.

CPUC is also developing a relationship with the California Department of General Services to implement federal expectations for Next Generation 9-1-1 enhancements for state of California.

Local Alerting and Warning Activity

(Gail used the power point prepared by Ron Alsop as a spring board for this section)

Overview

At the local government level, alert and warning options are varied and have mixed capabilities. There is the Emergency Alert System (EAS), with its short alert notification tones and messages that may be easily missed by the potential audience. Some jurisdictions use reverse "911" automatic dial/send systems. Recent events have highlighted issues with these systems; notification is not always received due to technical problems. The Emergency Digital Information Service (EDIS) is a system that relies on broadcasters and here again there are occasional technical difficulties, depending upon how the broadcast stations operate. A small number of locations use outdoor sirens as part of their alerting process. Testing the siren systems is frequently accompanied by "911" calls from people asking "Is this real? Is this a test?"

Some of these systems have their limitations. EAS provides an initial alert, but must be followed up with more detailed information from the media. Reverse 911 systems are basic and may not work for some categories of people, such as the hearing impaired or cellular-only customers, if the databases of numbers are not correct or residents have not "opted in". Outdoor sirens or voice systems are expensive and complicated to establish (and maintain). They require an ongoing public education campaigns and are generally limited to a specific threat and geographic area.

There are also lesser used methods of alert and warning, such as "tone alert" radios for key facilities, air craft or public safety vehicle mounted public address systems, and National Weather Radio (NWR).

Successful alert, warning, and notification present many challenges. The public must be educated on a continuous basis about the various systems, and, in a day and age of almost "instant information", the public has come to expect instant information about emergencies and disasters. Commercial radio and television stations in many areas are automated and there may be delays or elimination of live local disaster coverage.

There are other challenges as well, including:

- An inconsistent patchwork of systems;
- A lack of pre-scripted messages or the ability to develop on-the-spot information for the public;
- The problem of outdoor notifications, for transient populations such as campers, hikers, the homeless, etc.;
- Notification of those with special needs and vulnerabilities;

- The issue of multiple languages in California.

This section has provided a brief overview of alert, warning, and notification and the associated challenges. The recommendations in this Report will address these areas more fully and will reflect the efforts of the Working Group and key stakeholders.

Working Group Process

The process was initiated in March 2008 with the first meeting of the Alert and Warning Working Group (AWWG) held on March 27, 2008.   This "kick-off" meeting was the first in a series of meetings to implement the provisions of AB 2231 regarding enhancing alert, notification, and warning systems in California through public-private partnerships. The workshop focused on obtaining initial information to support AB 2331 implementation, identification of key stakeholders and interested parties, and outlining the process for implementing the project over the next year. At this meeting the participants also agreed to expand stakeholder participation as needed and identified the need to establish subcommittees ("work teams") to address key areas. Subsequent meetings expanded and extended the work begun in March 2008. These meetings were held June 24, 2008; September 2008 and December 2008. Summaries of the meetings are included in Appendix __ to this report.

As a result of the input received at the first meeting, five "Work Teams" were identified and formed. They are:

- Technical Issues,
- Social Issues,
- Standardization,
- Funding, and
- Legal and Liability Issues.

Subsequent to this initial identification of focus areas, it was suggested that the last two (Funding and Legal and Liability issues be merged for purposes of the initial issues identification. Several of the Work Teams discovered that they had overlapping areas of interest. *Where appropriate, the overlapping areas of interest are addressed in this report.*

The Work Teams began meeting in May 2008. The process used by the work teams were generally similar. The initial team meeting involved review of some preliminary information from the members regarding potential priority issues and other discussion areas. As a result of this meeting:

- some items were removed from the work teams area of responsibility;
- priority items were identified;
- a tentative work plan for the team was developed;
- the work team began initial issue recommendation development; and
- cross-cutting issues were identified that required joint work with other Work Teams

Throughout the year-long process, particular emphasis was placed on stakeholder involvement, at all levels of government, with the private sector (including vendors) and key nongovernmental organizations. For a listing of work team participants, see Appendix __ to this report.

Technical Issues

The work team agreed it should focus on issues at a policy level. For the report to the Legislature it will be important to identify the current status of alerting and warning technology in California and where the state needs to go.

There was general agreement that alerts and warnings are transmitted to multiple existing delivery systems which were not developed with alert and warning as a primary function nor to be an integrated system. Industry will play a huge role in this process, and if the industry is driving the technology, it is important that those representatives are heavily engaged in the work team's effort. However, the State's alert and warning system should not be technology driven but user driven (users should decide what the system is to accomplish and technology should support this.)

The work team began with the overall general assumption that whatever alert and warning system solutions are implemented, they must be consistent with the Common Alerting Protocol (CAP).

The following list summarizes the key issues identified by the work team. They are listed in the team's order of priority and critical statements within each section are identified in bold italics. .

Issue 1: Interface with Federal alert and warning systems and initiatives

As discussed in the previous section, improving national alert and warning capabilities is a key topic of discussion at the federal level***. However, there is a need for a clear definition of responsibilities at the State level for participation in federal activities; without this our voice won't be heard.*** The state's alerting and warning system will need to adapt to the changing federal landscape. However, because EDIS is CAP-compliant, this should be readily achievable. ***CMAS, the Federal cellular notification system initiative, has not been fully implemented yet but the work group agreed that State should not develop its own system in the mean time***.

Issue 2: The State's role in alert and warning technology – EDIS (Emergency Digital Information Service)

EDIS uses the Common Alerting Protocol that is the backbone of both the federal Emergency Alert System and CMAS efforts. As such, ***EDIS can be made to do all the things we need, but it will take more investment***. Also, EDIS does not exist as a defined "program" for the purpose of budgetary support. ***There is a need for defined ownership and support (programmatic and financial) for EDIS at the state level***. Although EDIS is a potentially powerful tool, there may be an overestimate of its current capabilities. EDIS needs to be made more redundant and existing shortfalls cannot be solved solely by buying new technology.

Although EDIS is operated by the State, the State is the governmental level least likely to issue an emergency alert. Most alerts are issued by local emergency managers, who understand the impacts that a specific hazard or event will have on the local community and can communicate to alert recipients the most appropriate actions to take. However, the State should continue to take the lead role in further development and maintenance of EDIS in order to assure a common statewide platform.

Issue 3: Origination & transmitting of alerts and warnings in alternative languages

This issue was also addressed by the Standardization and Social Issues work teams. With regard to Technical issues surrounding issuing alerts in multiple languages, there was a need for additional information on technologies that may be available for "automatic" translation of alert and warning messages. ***The work team knows of no automated translation technology that is "provable" enough to be used for public safety; the team identified a need to define performance standards that these systems would need to meet***. Translation could occur at the originator, middleware, or client level. The need for appropriate translation to multiple communities underscores the importance of having a system employing many different methodologies of dissemination.

Issue 4: Management of changing technical options

The state needs an operational alert and warning platform that can adapt to changing technology, both in terms of message input and for the end user (multiple outputs). The system must also be able to adapt to changes in protocols and procedures, evolving management structures, and the like. ***The system must be able to deliver a single message to various recipients through various media ("plug and play").*** The team thought that pursuing a common "exchange" (middleware) solution rather than emphasizing a "mesh" architecture solution may be the most readily achievable.

Issue 5: Alternative/emerging technology for special needs

Achieving accessibility of alert and warning messages by recipients with sensory disabilities is a distinctly different challenge from language translation. ***The team believes that sensory disability learning preferences may already have been defined and this research needs to be built into any alert and warning system solutions. There is a need for a solution that can take a single message and translate it accurately to multiple special needs delivery methods***.

Issue 6: Interface w/local alert and warning delivery systems

Most alerts and warnings are issued at the local government level. Many local governments have invested in various types of alert and warning technologies. ***The pending CA-OES contract to gather information on the various technologies currently in use and their capabilities will be valuable in designing a solution that can accommodate these prior investments. It reiterates the need for a "plug and play" solution***. EDIS has the capability to link with most of the existing alerting systems. Compiling the local survey information into a directory would be useful. ***Procedures and protocols for coordinating and reconciling alerts and warnings that impact multiple local jurisdictions are also needed***.

Issue 7: Identity management

Identity management addresses how authorized users (message originators and distributors) are identified, validated, and credentialed. ***There is an ongoing effort by with the Department of Homeland Security to develop and implement an identification (ID) "smart card"; use of this initiative to manage access to the alerting/warning system should be explored.*** For example, could the ID card serve as a keycard for the message originator to unlock access to the alert and warning system? ***There is a need to tie alert and warning credentialing to the overall National Incident Management System***

(NIMS) required credentialing effort. Alert and warning is not currently addressed in the NIMS Resource Typing system. Identity management is an overlapping issue with the Standardization and Social Issues work teams.

Another element related to identity management relates to validating the "legitimacy" of requests by warning system partners (e.g., telecommunications companies, broadcasters) for access into the disaster area (e.g., to repair tower sites), for logistical support (e.g., fuel for generators) and the like.

Issue 8: Alert message and network management

Procedures and protocols are needed to enable alerting entities to manage message generation and distribution in a way to best use network capacity and avoid call blocking due to congestion.

Additional issues raised by the larger Working Group

Several additional issues were raised at the June 24, 2008 meeting of the larger Alert and Warning Working Group. These included:

- It's important to keep in mind that there is a difference between "alert" and "information." Procedures and protocols for implementing the system should address both (e.g., the need to follow-up alerts with public information to provide supplemental/updated information.)

- An open architecture or "plug-n-play" based system will yield the best results. The key for the technology side is to keep it as simple as possible.

- Technology providers are going to have to think about back-up power in the event that there is a power failure. Redundancy is one of the biggest issues to be addressed. The CPUC has recently come out with a report on battery back-up power for cell towers. This may be a useful study to look at.

- Spam control and defense mechanisms need to be built in to all systems.

- The technology work group needs to consider infrastructure sustainability standards. The issue of functionality vs. community aesthetics has already proved to be a point of contention in some communities.

Additional issues referred by other Work Teams

Issue 9: Caller ID

Many customers now have caller identification (ID) systems that block anonymous calls. Considerations should be given to having a uniform caller ID (such as "CA Alert" or "000-000-0000") for all warning messages generated by the California alert system. This "brandable" identifier could be highlighted during public education campaigns. However, the Standardization Work Team was not certain if this would be achievable with current technology.